

REMARKS / ARGUMENTS

Reconsideration of the application is requested.

Claims 1-20 remain in the application. Claims 5 and 15 have been amended. Claims 1-4 have been withdrawn.

In the section entitled "Claim Rejections - 35 USC § 102" on pages 2-4 of the above-mentioned Office action, claims 5-10 and 13-20 have been rejected as being anticipated by Pedersen et al. (US Pat. No. 5,936,302) under 35 U.S.C. § 102(e).

The rejection has been noted and claims 5 and 15 have been amended in an effort to even more clearly define the invention of the instant application. Support for the changes is found on page 11, lines 13-16 of the specification.

Before discussing the prior art in detail, it is believed that a brief review of the invention as claimed, would be helpful.

Claims 5 and 15 call for, inter alia:

conductor tracks provided within respective ones of the part chips;

.
.
.

a determining device operatively connected to said receiving device, said determining device determining

that there is a damage to the multi-dimensionally constructed chip stack if the electrical signal cannot be received, said determining device ensuring deactivation of security-relevant functional components in the part chips upon determination of damage in the chip stack.

The invention of the instant application relates to a method and a device for securing a multi-dimensionally constructed chip stack. The object of the invention of the instant application is to ensure that the connections between individual part chips of the chip stack cannot be undone or detached without such damage being detected. This is especially of interest if physical attacks on critical security chips, such as smart cards, are being made by attempting to divide the chip stack in order to gain access to secure parts of the chip. Detection of such an attack is achieved by providing a continuous electrical signal path running through the part chips, which would be damaged in such an attack.

It is important for the invention of the instant application that the signal path is not accessible from the outside. Basically this means that it is not possible to short-circuit the signal path from the outside in order to avoid damage detection. This feature can be found in claims 5, 9, 13, 15, and 18-19 where it is repeatedly mentioned that the conductor tracks (LB1, LB2, LB3) run inside the part chips. The

description also supports this feature and points out that the conductor tracks are inside the part chips, that the meandering line is integrated into the chip composite and that the conductor tracks are buried under the surface of the part chips. It is also clearly shown in Figs. 1-5 that there is no access to the electrical signal path from the outside.

The second important aspect of the invention of the instant application is that if the electrical signal path is damaged in an attack, appropriate counter measures, such as preventing further operation of one or more functional components or deleting secret data, are taken. For the deactivation to be effective, a replacement of those deactivated components must not be allowed. Any such action would seriously undermine the desired security of the chip stack.

Pedersen et al. disclose a method and an apparatus for addressing die, as well as stacks of segments made of die. The object of Pedersen et al. is to provide access to a functioning die when an attempt is made to access a defective die. This is accomplished by electrically disconnecting the defective die and then re-routing the control lines to a redundant die in the stack using conductive epoxy.

Pedersen et al. differ from the invention of the instant application in at least two important aspects:

1) The stack connections of Pedersen et al. are accessible from the outside:

- The metal interconnects between the die are patterned on the surface of each segment and are not hidden as in the invention of the instant application.
- Bond pads on dies and segments are accessible for connecting to external circuits and control lines.
- Segments in a stack are electrically connected using electrically conductive epoxy traces along the edges of the stack as shown in Fig. 1 of Pedersen et al. and thus are accessible from outside.

In contrast to the invention of the instant application, all these stack connections can be easily bridged or manipulated in some way. As a result, there is no way that these connections could be used to secure the stack as is claimed in the instant application.

2) In Pedersen et al., it is possible to replace a component by another:

In case a component (in this case a die) in the chip stack is damaged, Pedersen et al. replace it with a replacement

die, the aim of which is to provide redundancy. However, disconnecting a component and then replacing it with another in order to resume operation presents a severe security risk. Components containing identification data could be easily swapped and used for fraud. Such a chip stack would not be secure at all. In contrast to Pedersen et al., the invention of the instant application does not provide for a replacement of defective components. Rather, if one component is removed, the electrical signal path running through all the components is irreparably destroyed and selected components are deactivated.

In summary, Pedersen et al. are concerned with redundancy while the invention of the instant application is concerned with security. It is clear that the structure proposed by Pedersen et al. cannot solve the problem of securing a chip stack as described in the invention of the instant application.

Clearly, Pedersen et al. do not show "conductor tracks provided within respective ones of the part chips; ... a determining device operatively connected to said receiving device, said determining device determining that there is a damage to the multi-dimensionally constructed chip stack if the electrical signal cannot be received, said determining

device ensuring deactivation of security-relevant functional components in the part chips upon determination of damage in the chip stack" as recited in claim 1 of the instant application.

It is accordingly believed to be clear that none of the references, whether taken alone or in any combination, either show or suggest the features of claims 5 and 15. Claims 5 and 15 are, therefore, believed to be patentable over Pedersen et al. and since all of the dependent claims are ultimately dependent on claims 5 or 15, they are believed to be patentable as well.

In the section entitled "Claim Rejections - 35 USC § 103" on pages 4-5 of the above-mentioned Office action, claim 11 has been rejected as being unpatentable over Pedersen et al. in view of Kumamoto et al. (US Pat. No. 5,196,920) under 35 U.S.C. § 103(a); claim 12 has been rejected as being unpatentable over Pedersen et al. in view of Chen et al. (US Pat. No. 5,106,773) under 35 U.S.C. § 103(a).

As discussed above, claim 5 is believed to be patentable over the art. Since claims 11-12 are dependent on claim 5, they are believed to be patentable as well.

In view of the foregoing, reconsideration and allowance of claims 5-20 are solicited. Rejoinder of method claims 1-4 is requested upon allowance of product claims 5-20.

In the event the Examiner should still find any of the claims to be unpatentable, counsel would appreciate a telephone call so that, if possible, patentable language can be worked out.

If an extension of time for this paper is required, petition for extension is herewith made. Please charge any fees which might be due with respect to 37 CFR Sections 1.16 and 1.17 to the Deposit Account of Lerner and Greenberg, P.A., No. 12-1099.

Respectfully submitted,

LAURENCE A. GREENBERG
REG. NO. 29,308



For Applicants

YC

May 26, 2004

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101